REMARKS

Reconsideration of this Application is respectfully requested. In response to the Office Action mailed December 2, 2004, Applicant has amended the specification, and claims 1, 14, 27, 36, and 42. Claims 1-55 are pending.

Based on the above Amendment and the following Remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Objections to the Specification

On page 2, the Action objects to the specification because of informalities.

Accordingly, Applicant has corrected the informalities on page 4, lines 8 and 14, and on page 8, lines 13-14 as suggested in the Action. Applicant respectfully requests that the objection be withdrawn.

Rejections under 35 U.S.C. § 102

On pages 2-7, the Action rejects claims 1, 4, 11, 14, 17, 19, 27, and 36 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2002/0101989 A1 to Markandey et al. (hereinafter Markandey). Applicant respectfully disagrees.

(a) On page 3, the Action rejects claim 1 under 35 U.S.C. § 102(e) as being anticipated by Markandey.

Amended claim 1 recites: "A method for securely transmitting data comprising: obtaining non-packetized data on a computer system for transmission; **encrypting the data a first time** such that the data is once encrypted; packetizing the once encrypted data; encrypting the

packetized, once encrypted data a second time such that the data is twice encrypted; and

transmitting the packetized, twice encrypted data." (emphasis added).

In contrast, Markandey discloses a DVD system for communicating between a

transmitter and a receiver. In FIG. 7, Markandey discloses the transmitter reading scrambled

data that is **stored** on a DVD along with a corresponding Scramble_Pattern_ID of Texas

Instruments Registration and Identification System (TIRIS) (see Markandey, FIG. 7, paragraph

[0075]). The scrambled data and the Scramble_Pattern_ID are then packaged into IEEE 1394

packets for transmission on a IEEE 1394 medium (see Markandey, FIG. 8, paragraph [0075]).

After the data is combined into IEEE 1394 packets, the data is encrypted and then transmitted on

the IEEE 1394 medium (see Markandey, paragraph [0076]). The preferred encryption of this

system is implemented using the Data Encryption Standard (DES), which encrypts 64-bit blocks

of data using a 64-bit session key to produce a 64-bit encrypted result (see Markandey, paragraph

[0025]). At the receiver, the data is received from the IEEE 1394 medium, decrypted, and

unpacked (see Markandey, paragraph [0076]). The Scramble_Pattern_ID is used to index a

lookup table to descramble the scrambled data at the receiver (see Markandey, Table 5,

paragraph [0076]).

For at least the following two reasons, Markandey does not anticipate the features recited

in claim 1.

First, Markandey does not teach or suggest "**encrypting the data a first time** such that

the data is once encrypted," as recited in claim 1. On page 3, lines 7-8, the Action states that the

claimed "encrypting data for a first time" is anticipated by the reference "DVD" of FIG. 7 from

Markandey. In FIG. 7, Markandey discloses a transmitter that **reads** scrambled data from a

DVD along with a Scramble_Pattern_ID (see Markandey, paragraph [0075]), but does not

disclose that the transmitter **encrypts** the data read from the DVD for a first time. Instead, the scrambled data of Markandey is **stored** on the DVD itself (see Markandey, paragraph [0075]). Thus, the transmitter does not perform scrambling. Since the transmitter of Markandey does not performing a step of scrambling data, it also does not include a step of "encrypting the data for a first time," and thus the transmitter does not anticipate this feature in claim 1. Therefore, Markandey does not anticipate claim 1.

Second, encryption and scrambling are different processes according to Markandey. On page 3, lines 7-8, the Action states the claimed step of "encrypting the data for a first time" is anticipated by the scrambled data in FIG. 7 of Markandey. However, in the description, Markandey distinguishes between encryption and scrambling. Specifically, Markandey describes the encryption process as encoding data using the Data Encryption Standard (DES), which encrypts 64-bit blocks of data using a 64-bit session key to produce a 64-bit encrypted result (see Markandey, paragraph [0025]). Thus, Markandey describes encryption as a process of encoding data using a key. In contrast, Markandey describes scrambling as interchanging the order of various digital bits according to a scramble pattern, and provides examples of various scramble patterns in Table 5 (see Markandey, paragraph [0071]). Clearly, Markandey does not consider encryption equivalent to scrambling. Thus, scrambling is not the same as or equivalent to encryption in the system of Markandey. Therefore, even if Markandey taught scrambling as a step in his process, this reference would not anticipate claim 1 since scrambling is not equivalent to encryption according to Markandey.

Accordingly, claim 1 is allowable over the cited prior art and allowance thereof is respectfully requested.

Claims 4 and 11, which depend directly and indirectly from claim 1, are also in condition for allowance because of their dependence on an allowable claim.

(b) On pages 3-4, the Action rejects claim 14 under 35 U.S.C. § 102(e) as being anticipated by Markandey.

Amended claim 14 recites: "A method for securely receiving data comprising: **receiving packetized, twice encrypted data**; decrypting the packetized, twice encrypted data a first time such that the packetized data is once decrypted; reconstructing the non-packetized, once decrypted data; and decrypting the reconstructed, once decrypted data a second time." (emphasis added).

For at least the following two reasons, Markandey does not teach or suggest all of the features of claim 14.

First, Markandey does not teach or suggest "receiving packetized, twice encrypted data," as recited in claim 14. On page 3, line 16, the Action states that the receiver of Markandey in FIG. 7 anticipates the claimed step of "receiving packetized, twice encrypted data." However, for reasons discussed above, Markandey does not disclose a transmitter that sends twice encrypted data. Instead, the data transmitted to the receiver in FIG. 7 of Markandey is only **once** encrypted (see Markandey, paragraphs [0075]-[0076]). This means that the receiver of Markandey does not receive twice encrypted data. Thus, Markandey does not teach or suggest or suggest "receiving packetized, twice encrypted data," as recited in claim 14. Therefore, Markandey does not anticipate claim 14.

Second, Markandey does not teach or suggest "**reconstructing** the non-packetized, once decrypted data; and **decrypting** the reconstructed, once decrypted data a second time," as recited in claim 14 as amended. Markandey only discloses a single decryption and a single

descrambling (see Markandey, paragraphs [0075]-[0076]), but does not disclose a second

decryption. As discussed above, Markandey distinguishes between scrambling and encryption,

which implies that descrambling at the receiver in Markandey is not equivalent to decryption.

Also, the only decryption discussed in Markandey is on data in IEEE 1394 packets (see

Markandey, paragraph [0076]); however, Markandey does not disclose decryption of

reconstructed, **non-packetized**, once decrypted data. Thus, Markandey does not teach or suggest

or suggest "**reconstructing** the non-packetized, once decrypted data; and decrypting the

reconstructed, once decrypted data a second time," as recited in claim 14 as amended.

Therefore, Markandey does not anticipate claim 14. Applicant respectfully requests that the

rejection be withdrawn.

Accordingly, claim 14 is in condition for allowance and allowance thereof is respectfully

requested.

Claims 17 and 19, which depend directly and indirectly from claim 14, are also in

condition for allowance because of their dependence on an allowable claim.

(c) On pages 4-6, the Action rejects claims 27 and 36 under 35 U.S.C. § 102(e) as being

anticipated by U.S. Patent No. 5,721,778 to Kubota (hereinafter Kubota). However, this

reference to Kubota appears to be erroneous. The rejection applied in the Action appears to be

based on Markandey as the figures referenced and described on pages 4-6 of the Action refer to

Markandey, and do not correspond to Kubota. Applicant will assume the Action intended to

refer to Markandey, and not Kubota.

(i) Amended claim 27 recites: "A method for securely transmitting and receiving data

comprising: obtaining non-packetized data on a first computer system for transmission;

encrypting the data a first time such that the data is once encrypted; transmitting the once

encrypted data from the first computer system to a first interface device; receiving the once

encrypted data at the first interface device; packetizing the once encrypted data; encrypting the

packetized, once encrypted data a second time such that the data is twice encrypted; and

transmitting the packetized, twice encrypted data from the first interface device to a second

interface device; receiving packetized, twice encrypted data at the second interface device;

decrypting the packetized, twice encrypted data a first time such that the packetized data is once

decrypted; reconstructing the packetized, once decrypted data; transmitting the reconstructed,

once decrypted data from the second interface device to a second computer system; receiving the

reconstructed, once decrypted data at the second computer system; and decrypting the

reconstructed, once decrypted data a second time." (emphasis added).

On page 4, the Action identifies the scrambled data from FIG. 7 of Markandey as

anticipating the claimed step of "encrypting the data a first time such that the data is once

encrypted." However, for reasons analogous to those given in the remarks on claim 1,

Markandey does not teach a first encryption (or scrambling) step of data read from the DVD, nor

does Markandey consider scrambling to be equivalent to encryption. Thus, Markandey does not

anticipate claim 27 and the rejection of claim 27 is improper. Applicant respectfully requests

that the rejection be withdrawn.

Accordingly, claim 27 is in condition for allowance and allowance thereof is respectfully

requested.

(ii) For reasons analogous to those given for claims 1, 14, and 27, Markandey does not

anticipate amended claim 36. Applicant respectfully requests that the rejection be withdrawn.

Accordingly, claim 36 is in condition for allowance and allowance thereof is respectfully

requested.

Rejections under 35 U.S.C. § 103

On pages 7-14, the Action rejects claims 2, 3, 10, 12, 13, 15, 16, 18, 24, 26, 28-35, 37-45, 47-51, and 53-55 under 35 U.S.C. § 103(a) as being obvious over Markandey in view of U.S. Patent No. 6,542,992 to Peirce, Jr. et al (hereinafter Peirce, Jr.). Applicant respectfully disagrees.

(a) As discussed above, claim 1 is in condition for allowance. Claims 2, 3, 10, 12, and 13 which depend directly and indirectly from allowable claim 1, are also in condition for allowance because of their dependence on an allowable claim.

(b) As discussed above, claim 14 is in condition for allowance. Claims 15, 16, 18, 24, and 26, which depend directly and indirectly from allowable claim 14, are also in condition for allowance because of their dependence on an allowable claim.

(c) As discussed above, claim 27 is in condition for allowance. Claims 28-35, which depend directly and indirectly from allowable claim 27, are also in condition for allowance because of their dependence on an allowable claim.

(d) As discussed above, claim 36 is in condition for allowance. Claims 37-41, which depend directly and indirectly from claim 36, are also in condition for allowance because of their dependence on an allowable claim.

(e) On pages 8-9, the Action rejects claim 42 under 35 U.S.C. § 103(a) as being obvious in view of the combination of Markandey with Peirce, Jr. et al.

Amended claim 42 recites: "A method for transmitting secure data comprising: **encrypting non-packetized data at a data link layer**; packetizing the data; encrypting the

packetized data at an Internet Protocol layer; and transmitting the packetized, encrypted data over a network." (emphasis added).

Applicant respectfully traverses the rejection as the Action fails to establish a *prima facie* case of obviousness. In order to establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. M.P.E.P. § 2143.

Applicant contends that the Action does not establish a *prima facie* case of obviousness for at least the following three reasons.

First, the combination of Markandey with Peirce, Jr. does not teach or suggest all of the claim features in claim 42. Particularly, neither disclose "encrypting the non-packetized data at a data link layer," (emphasis added) as recited in claim 42. As discussed above with reference to the remarks on claim 1, Markandey discloses reading scrambled data from a DVD (see Markandey, FIG. 7, paragraphs [0076]-[0077]), and does not disclose a first scrambling or a first encryption of the scrambled data read from the DVD. Similarly, Peirce, Jr. does not disclose the claimed feature. The only reference to the data link layer in Peirce, Jr. is in column 5, lines 27-30 in reference to the Point-to-Point protocol (PPP). However, as is known to those in the art, PPP is a **packetizing protocol**. Markandey and Peirce, Jr. only describe encryption on packetized data. Thus, neither Markandey nor Peirce, Jr. disclose "encrypting the non-packetized data at a data link layer," (emphasis added) as recited in claim 42. Therefore, the rejection over the combination of Markandey with Peirce, Jr. is improper.

Second, one of ordinary skill in the art would not be motivated to combine Markandey

with Peirce, Jr. to render obvious claim 42, as suggested in the Action, since these references

describe systems related to different technologies. Markandey describes a system to protect

DVD data on an IEEE 1394 bus. The system of Markandey reads scrambled data from a DVD,

places the scrambled data into IEEE 1394 isochronous packets, and then encrypts the IEEE 1394

isochronous packets for transmission across an IEEE 1394 bus (see Markandey, paragraph

[0076]-[0077]). However, Markandey does not teach or suggest that the scrambled data read

from the DVD may be encrypted on a first network layer and does not teach or suggest that the

encryption of the IEEE 1394 packets is on a second network layer. Applicant notes that

Markandey describes multiple protection layers (see Markandey, paragraph [0021]), but this

does not refer to encryption across multiple network layers as in standard networking protocols,

such as the Open System Interconnection (OSI) Model. Rather, the term "layer" in Markandey

is used to refer to a combination of different ways to protect data. For example, one protection

layer is to encrypt IEEE 1394 isochronous packets, a second layer is to scramble (rearrange) bits

in a packet header, and a third layer of reading scrambled stored data from a DVD (see

Markandey, paragraphs [0021], [0061]-[0069], and [0069]-[0074]). Although Markandey

references TCP/IP networks in paragraph [0099], the disclosed system "introduces to 1394

communication cryptographic techniques that have been used in . . . TCP/IP networks" and does

not state that reading the scrambled data and encrypting the IEEE 1394 packets occurs on

separate network layers.

In contrast with Markandey, Peirce Jr. describes a system that prevents unnecessary

duplication of encryption and compression by two different network entities at both the Point-to-

Point Protocol (PPP) layer and the Internet Protocol (IP) layer (see Peirce, Jr., Abstract, col. 2,

lines 18-32). The system of Peirce, Jr. does not describe applying this technology to IEEE 1394

systems. The Action does not provide any reasoning as to why one of ordinary skill in the art

would combine an IEEE 1394 system using only a single encryption of data transmitted across

an IEEE 1394 bus that does not use or even mention encrypting on either of the data link layer or

on the IP layer, as described in Markandey, with a system that prevents unnecessary duplication

of encryption at the PPP layer and at the IP layer on a non-IEEE 1394 system, as described in

Peirce, Jr. The description of encrypting data across different network protocol layers described

in Peirce. Jr. is not relevant to sending once encrypted data across an IEEE 1394 bus in the

Markandey reference. Thus, one of ordinary skill in the art would not be motivated to combine

Markandey with Peirce, Jr. because they describe non-analogous systems, and there is no reason

to combine these distinct technologies. Therefore, the rejection of claim 42 as being obvious in

light of a combination of these references is improper.

Third, the Action does not identify proper motivation for combining Markandey with

Peirce, Jr. On page 9 lines 4-6, the Action states:

> "It would have been obvious to one having ordinary skill in the art, at the time the
> invention was made, to introduce two layers coordination and encryption techniques and
> using the internet as the method of communicating as per teaching of Peirce in to the
> method of as taught by Markandey, in order to avoid ***unnecessary duplication*** of
> encryption at different layers, <u>ensure a more firmly security and provide secure services
> over the internet</u>."

Applicant respectfully disagrees.

The motivation to combine stated in the Action only applies to the Peirce, Jr. reference,

and is not relevant to the Markandey reference for at least the following two reasons.

(I) The motivation suggested in the Action is motivation **not** to combine Markandey with

Peirce, Jr. to render the claimed invention obvious. The Action states the motivation to combine

is "to avoid *unnecessary* duplication of encryption at different layers" (emphasis added) on page

9. Since the Action interprets reading scrambled data from a DVD as encryption in Markandey

(see at least page 8), the Action interprets Markandey as applying multiple encryptions to the

scrambled data. However, the Action's interpretation of Markandey as performing multiple

encryptions would lead one of ordinary skill in the art not to combine Markandey with a system

that is designed to **avoid** a duplication of encryptions, such as that disclosed by Peirce, Jr. (see

Peirce, Jr. col. 4, lines 13-55). The combination proposed in the Action would only have a

single encryption in order to "avoid *unnecessary* duplication of encryption at different layers,"

and thus would not teach or suggest all of the features in claim 42, which requires a method that

encrypts at both the Internet Protocol layer and at the data link layer (see claim 42, lines 2 and 4).

Using the Action's reasoning of avoiding unnecessary duplication of encryption, Peirce, Jr.

teaches away from being combined with the system of Markandey. Thus, one of ordinary skill in

the art would not be motivated to combine Markandey with Peirce, Jr. because of the motivation

from Peirce, Jr. not to combine, as stated in the Action.

(II) The motivation stated by the Action also provides further reasoning for not

combining Markandey with Peirce, Jr. On page 9, the Action states that adding additional

security to provide secure services for data transmission across the internet as motivation for

combining Markandey with Peirce, Jr. However, securely transmitting services across the

internet is irrelevant to the system of Markandey since the data transmitted in Markandey is

across an IEEE 1394 bus, and not across the internet (see Markandey, paragraph [0003]).

Although Markandey references TCP/IP networks in paragraph [0099], this reference does not

state that the disclosed system transports data across the internet. Rather, Markandey states that

the disclosed system "introduces to 1394 communication cryptographic techniques that have

been used in . . . TCP/IP networks." One of ordinary skill in the art would not be motivated to combine Markandey with Peirce, Jr. to "ensure a more firmly security and provide secure services over the **internet**" (emphasis added) since Markandey does not transmit data over the internet. Thus, there is no motivation to combine Markandey with Peirce, Jr., as suggested in the Action. Therefore, the Action does not establish a *prima facie* case of obviousness for combining Markandey with Peirce, Jr., and the rejection of claim 42 is improper. Applicant respectfully requests that the rejection be withdrawn.

Accordingly, claim 42 is in condition for allowance and allowance thereof is respectfully requested.

Claim 43, which depends directly from claim 42, is also in condition for allowance because of its dependence on an allowable claim.

(f) On page 8, the Action rejects claim 44 under 35 U.S.C. § 103(a) as being obvious in view of the combination of Markandey with Peirce, Jr.

Claim 44 recites: "A method for transmitting secure data comprising: encrypting the data at an Internet Protocol layer; further encrypting the encrypted data at a data link layer; and transmitting the data over a communication link."

For at least the following reasons, the combination of Markandey with Peirce, Jr. does not teach all of the features of claim 44.

The combination of Markandey with Peirce, Jr. does not teach or suggest "further encrypting the encrypted data at a data link layer," as recited in claim 44. This process is described on, for example, page 13, lines 15-29 of the instant application. In this embodiment, the data processed at the link layer is a bit stream, and is not packetized. Thus, the claimed step of "further encrypting the encrypted data at a data link layer" is on non-packetized data. For

25

reasons discussed above in the remarks on claim 42, the combination of Markandey with Peirce, Jr. only discloses encryption on packetized data, and does not teach or suggest this feature of encryption on a bit stream at the data link layer. Also, as discussed above in the remarks on the rejection of claim 42, there is no motivation to combine Markandey with Peirce Jr. to render claim 44 obvious. Therefore, the Action does not establish a *prima facie* case of obviousness for combining Markandey with Peirce, Jr., and the rejection of claim 44 is improper. Applicant respectfully requests that the rejection of claim 44 be withdrawn.

Accordingly, claim 44 is in condition for allowance and allowance thereof is respectfully requested.

Claims 45 and 47-49, which depend directly and indirectly from claim 44, are also in condition for allowance because of their dependence on an allowable claim.

(g) On page 9, the Action rejects claim 50 under 35 U.S.C. § 103(a) as being obvious in view of the combination of Markandey with Peirce, Jr.

Claim 50 recites: "A method for receiving secure data comprising: receiving the data over a communication link; decrypting the data at a data link layer; and further decrypting the decrypted data at an Internet Protocol layer."

For reasons similar to those given for claim 44, the combination of Markandey with Peirce, Jr. does not teach or suggest "decrypting the data at a data link layer," and there is no motivation to combine Markandey with Peirce Jr. to render claim 50 obvious. Therefore, the Action does not establish a *prima facie* case of obviousness for combining Markandey with Peirce, Jr., and the rejection of claim 50 is improper. Applicant respectfully requests that the rejection of claim 50 be withdrawn.

Accordingly, claim 50 is in condition for allowance and allowance thereof is respectfully requested.

Claims 51 and 53-55, which depend directly and indirectly from allowable claim 50, are also in condition for allowance because of their dependence on an allowable claim.

(h) On pages 14-16, the Action rejects claims 5-8 and 20-23 under 35 U.S.C. § 103(a) as being obvious over Markandey in view of European Patent No. 0 406 187 A1 to Blom (hereinafter Blom). Applicant respectfully disagrees.

As discussed above, claim 1 is in condition for allowance. Claims 5-8, which depend directly and indirectly from allowable claim 1, are also in condition for allowance because of their dependence on an allowable claim.

As discussed above, claim 14 is in condition for allowance. Claims 20-23, which depend directly and indirectly from allowable claim 14, are also in condition for allowance because of their dependence on an allowable claim.

(i) On pages 16-17, the Action rejects claims 9 and 25 under 35 U.S.C. § 103(a) as being obvious over Markandey in view of U.S. Patent No. 6,697,872 to Moberg (hereinafter Moberg). Applicant respectfully disagrees.

As discussed above, claim 1 is in condition for allowance. Claim 9, which depends directly from allowable claim 1, is also in condition for allowance because of its dependence on an allowable claim.

As discussed above, claim 14 is in condition for allowance. Claim 25, which depends directly from allowable claim 14, is also in condition for allowance because of its dependence on an allowable claim.

(j) On pages 17-18, the Action rejects claims 46 and 52 under 35 U.S.C. § 103(a) as being obvious over Markandey in view of Peirce, Jr. and further in view of Moberg. Applicant respectfully disagrees.

As discussed above, claim 44 is in condition for allowance. Claim 46, which depends directly from allowable claim 44, is also in condition for allowance because of its dependence on an allowable claim.

As discussed above, claim 50 is in condition for allowance. Claim 52, which depends directly from allowable claim 50, is also in condition for allowance because of its dependence on an allowable claim.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed,

accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner

reconsider all presently outstanding objections and rejections and that they be withdrawn.

Applicant believes that a full and complete reply has been made to the outstanding Office Action

and, as such, the present application is in condition for allowance. If the Examiner believes, for

any reason, that personal communication will expedite prosecution of this application, the

Examiner is hereby invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment is respectfully requested.

Respectfully submitted,

Date: June 1, 2005

Edward W. Yee
Registration No. 47,294
VENABLE LLP
P.O. Box 34385
Washington, D.C. 20043-9998
Telephone: (202) 344-4000
Telefax: (202) 344-8300

DC2-DOCS1-651232